THERE ARE SALEM NUMBERS OF EVERY TRACE

JAMES MCKEE AND CHRIS SMYTH

Abstract. We show that there are Salem numbers of every trace. The nontrivial part of this result is for Salem numbers of negative trace. The proof has two main ingredients. The first is a novel construction, using pairs of polynomials whose zeros interlace on the unit circle, of polynomials of specified negative trace having one factor a Salem polynomial, with any other factors being cyclotomic. The second is an upper bound for the exponent of a maximal torsion coset of an algebraic torus in a variety defined over the rationals. This second result, which may be of independent interest, enables us to refine our construction to avoid getting cyclotomic factors, giving a Salem polynomial of any specified trace, with a trace-dependent bound for its degree.

We show also how our interlacing construction can be easily adapted to produce Pisot polynomials, giving a simpler, and more explicit, construction for Pisot numbers of arbitrary trace than previously known.

1. Introduction

A *Salem number* is an algebraic integer greater than 1 whose other conjugates all lie in the closed disc $|z| \leqslant 1$, with at least one on $|z| = 1$. Our main result is the following.

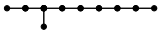
Theorem 1. *For every negative integer $-T$ there is a Salem number of trace $-T$ and degree at most* $\exp\exp(22 + 4T\log T)$.

It is easy to produce Salem numbers of any nonnegative trace, so the title of the paper is justified. The interest in this result is that, until now, all Salem numbers found had trace no smaller than -1 ([19]). Furthermore, it is now known that a Salem number of degree $d \geqslant 10$ has trace at least $\lfloor 1 - d/9 \rfloor$, and it seemed conceivable that there was a finite lower bound for the trace. For more details see the end of the paper.

To provide a little background, we give a brief sketch of some facts about Salem numbers. The minimal polynomial $P(z)$ of a Salem number τ is *reciprocal*, that is, it satisfies $z^{\deg P}P(1/z) = P(z)$, so that τ^{-1} is a conjugate of τ, and the coefficients of P are "palindromic". All conjugates of τ apart from τ and τ^{-1} lie on $|z| = 1$, and $P(z)$ has even degree. For every $\varepsilon > 0$ and Salem number τ there is a $\lambda \in \mathbb{Q}(\tau)$ such that for $k = 0, 1, 2 \ldots$ all $\lambda\tau^k$ have distance at most ε from an integer. If a number field K contains a Salem number τ of full degree $[K : \mathbb{Q}]$ then every full degree Salem number in K is a power of the smallest such Salem number in K. It is not known whether there are Salem numbers arbitrarily close to 1. If "Lehmer's conjecture" is true, then there are not. The smallest known Salem number $1.176280818\cdots$, discovered by Lehmer in 1933, has minimal polynomial

Date: 19 Feb 2004.

2000 *Mathematics Subject Classification.* Primary 11R06.

$L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$. The polynomial $L(-z)$ had just appeared (in 1932) in Reidemeister's book [15] as the Alexander polynomial of a pretzel knot. For recent connections with knot theory, see E. Hironaka [9]. The polynomial $L(z)$ can also be obtained from the characteristic polynomial $E_{10}(x)$ of the (adjacency matrix of the) Coxeter graph $E_{10} =$  by the transformation $L(z) = z^5 E_{10}(z^{1/2} + z^{-1/2})$. There are currently 47 known Salem numbers less than 1.3 (see Mossinghoff [11]).

Salem numbers are closely related to Pisot numbers, which are much better understood. A *Pisot number* is an algebraic integer greater than 1 whose other conjugates all lie in the open disc $|z| < 1$. For every Pisot number θ, the distance of θ^n from the nearest integer tends to 0 as $n \to \infty$. The set of all Pisot numbers is a closed subset of the real line. Every Pisot number is a limit point of Salem numbers, and Boyd [4, p. 327] has conjectured that Pisot numbers are the only limit points of Salem numbers. If this is true, then the set of all Pisot and Salem numbers is also closed. See Bertin *et al* [1], Boyd [4, 5], Ghate and Hironaka [7] and Salem [17] for these and other results about Salem and Pisot numbers.

It is already known (see [14, 12]) that there are Pisot numbers of every trace. However, we can greatly reduce the known upper bound for the smallest degree of a Pisot number of given negative trace.

Theorem 2. *For every negative integer $-T$ there is a Pisot number of trace $-T$ and degree at most the sum of the first $2T + 4$ primes.*

This sum is asymptotic to $2T^2 \log T$. The simple examples $z^3 - z - 1$, $z^2 - z - 1$ and $z - n\,(n \geqslant 2)$ of minimal polynomials of Pisot numbers then show that there are Pisot numbers of every trace.

Computations for negative trace down to -25 (see Section 8) indicate that the upper bound on the degree in Theorem 1 should be comparable with that in Theorem 2. However, a proof of this does not seem within reach at present.

In [14], for infinitely many degrees d the existence of a Pisot number of degree d and trace $< \frac{-\log d}{4(\log\log d)^{3/2}}$ was proved. Theorem 2 improves this bound to $-c\sqrt{d}/\log d$ for some positive constant c.

One ingredient needed for the proof of Theorem 1 is a result concerning the exponent of maximal torsion cosets on a variety (Theorem 8), which may be of independent interest.

To end the introduction, we mention one immediate consequence of Theorem 1.

Corollary 3. *For infinitely many n there is a totally positive algebraic integer of degree n and trace less than $2n - \frac{1}{4}\log\log n/\log\log\log n$.*

This follows easily from Theorem 1, using the fact that $\tau + 1/\tau + 2$ is totally positive for any Salem number τ.

2. **Outline of the proof**

There are two main ingredients in the proof of Theorem 1. The first is a new construction for Salem numbers, which uses pairs of polynomials whose zeros interlace on the unit circle. It is an extension of the Salem number construction method used in [14], where

the interlacing polynomials arose from star-like trees. This new construction produces a polynomial of any specified negative trace that is, up to a possible cyclotomic factor, the minimal polynomial of a Salem number (or a reciprocal Pisot number).

The purpose of the second ingredient is to get rid of the possibility of a cyclotomic factor, while at the same time bounding the degree of the Salem number. It is based on ideas of Schmidt [18], and gives an upper bound for the exponent of a maximal torsion coset on a variety. This result is applied to a particular hypersurface to prove that the parameters in our polynomial construction can be chosen so that the polynomial in fact has no cyclotomic factor. This gives us our Salem number of the specified trace, with a bound on its degree.

3. **Construction of Salem and Pisot numbers by interlacing**

Lemma 4. *Suppose that* $\gamma > 0$, $\alpha_1 < \beta_1 < \alpha_2 < \cdots < \beta_{d-1} < \alpha_d \leqslant A$, *and*

$$f(x) := \frac{\gamma \prod_{j=1}^{d-1}(x-\beta_j)}{\prod_{j=1}^{d}(x-\alpha_j)}. \tag{1}$$

Then $f(x)$ *can be written as*

$$f(x) = \sum_j \frac{\lambda_j}{x-\alpha_j}, \quad \text{with } \lambda_j > 0 \quad \text{for all } j. \tag{2}$$

Further, the equation $f(x) = 1$ *has real roots* $\gamma_1, \ldots, \gamma_d$, *where* $\alpha_1 < \gamma_1 < \beta_1 < \alpha_2 < \gamma_2 < \beta_2 \cdots < \gamma_{d-1} < \beta_{d-1} < \alpha_d < \gamma_d$. *Also* $\gamma_d > A$ *if and only if* $f(A) > 1$.

Conversely, every $f(x)$ *of the form (2) can be written in the form (1) for some* $\gamma > 0$ *and* $\beta_1, \ldots, \beta_{d-1}$ *that interlace with the* α_j.

Proof. The interlacing condition for the roots easily implies (2). Then the results follow immediately on applying the Intermediate Value Theorem to $\sum_j \frac{\lambda_j}{x-\alpha_j}$. □

We say that a pair of relatively prime polynomials p and q satisfy the *circular interlacing condition* if they both have real coefficients, positive leading term, and all their zeros lie on the unit circle, and interlace there. This last condition means that, progressing clockwise around the unit circle, a zero of p and a zero of q are encountered alternately. Thus p and q have the same degree, and neither has a multiple zero. Note too that if p and q satisfy the circular interlacing condition, so do $p(z^n)$ and $q(z^n)$ for $n = 1, 2, \ldots$. In particular, the pair $z^n - 1$ and $z^n + 1$ satisfy it.

Pisot numbers whose minimal polynomials are reciprocal behave in some ways like Salem numbers. It is clear that they must be quadratic.

Proposition 5. *Suppose that the polynomials* p *and* q *satisfy the circular interlacing condition, have integer coefficients, and that* p *is monic (and thus cyclotomic). Then*

(a) *if* $p(1) = 0$, *or* $q(1) = 0$ *and* $2p(1) - q'(1) < 0$, *then* $(z^2-1)p(z) - zq(z)$ *is the minimal polynomial of a Salem number (or perhaps a reciprocal Pisot number), possibly multiplied by a cyclotomic polynomial. [Note: one of* $p(1)$ *and* $q(1)$ *is always* 0.*]*

(b) *always* $(z^2-z-1)p(z)-zq(z)$ *is the minimal polynomial of a Pisot number.*

Proof. Firstly, it is clear that, as the zeros of p and q interlace, both 1 and -1 must be zeros of pq, all other zeros of both p and q occurring in complex conjugate pairs. Put $z+1/z=x$, real and in $[-2,2]$ for z on the unit circle.

(a) Let γ be the leading coefficient of q.

Suppose first that p and q have even degree $2d$. If z^2-1 divides q, then

$$f(x) := \frac{z}{z^2-1}\cdot\frac{q(z)}{p(z)} = \frac{\gamma\prod_{j=1}^{d-1}(x-\beta_j)}{\prod_{j=1}^{d}(x-\alpha_j)}, \tag{3}$$

where the $\alpha_j = r_j + 1/r_j$, $\beta_j = s_j + 1/s_j$ for zeros r_j of p, s_j of q, and

$$-2 < \alpha_1 < \beta_1 < \alpha_2 < \cdots < \beta_{d-1} < \alpha_d < 2.$$

Thus, by Lemma 4, this quotient is equal to $\sum_j \frac{\lambda_j}{x-\alpha_j}$ for some $\lambda_j > 0$. On the other hand, if z^2-1 divides p, then

$$\frac{z}{z^2-1}\cdot\frac{q(z)}{p(z)} = \frac{\gamma\prod_{j=1}^{d}(x-\beta_j)}{(x^2-4)\prod_{j=1}^{d-1}(x-\alpha_j)},$$

with

$$-2 < \beta_1 < \alpha_1 < \beta_2 < \cdots < \alpha_{d-1} < \beta_d < 2.$$

Thus Lemma 4 can be applied again to give the same conclusion.

Now suppose that p and q have odd degree $2d+1$. Then for ε equal to one of ±1, $(z-\varepsilon)$ divides q and $(z+\varepsilon)$ divides p. Then

$$\frac{z}{z^2-1}\cdot\frac{q(z)}{p(z)} = \frac{\gamma\prod_{j=1}^{d}(x-\beta_j)}{(x+2\varepsilon)\prod_{j=1}^{d}(x-\alpha_j)},$$

and

$$-2 < \beta_1 < \alpha_1 < \beta_2 < \cdots < \beta_d < \alpha_d < 2 \quad \text{for } \varepsilon = 1$$
$$-2 < \alpha_1 < \beta_1 < \alpha_2 < \cdots < \alpha_d < \beta_d < 2 \quad \text{for } \varepsilon = -1$$

so that again Lemma 4 applies.

Now one of $\{p(1), q(1)\}$ is zero and the other positive, and $(z^2-1)p(z)-zq(z)$ is the numerator of $1-f(x)$. Hence the conditions given at $z=1$ are clearly those necessary and sufficient for $(z^2-1)p(z)-zq(z)$ to have a real zero greater than 1.

(b) We consider the sum

$$\frac{q(z)}{p(z)} + \frac{z^n+1}{z^n-1}$$

and write its uncancelled numerator and denominator as $q^*(z)g(z)$ and $p^*(z)g(z)$ respectively, where q^* and p^* are relatively prime. Then, because the pairs $\{q,p\}$ and $\{z^n+1, z^n-1\}$ satisfy the circular interlacing condition, so do q^* and p^*, by Proposition 6. (Note that there is no circularity, as the proof of Proposition 6 uses only part (a) of this proposition.) Then $g(z)((z^2-1)p^*-zq^*) = z^n((z^2-z-1)p-$

$zq)-(z^2+z-1)p+zq$ is of the form $z^n R(z) \pm R^*(z)$, where $R(z) = (z^2-z-1)p-zq$ and $R^*(z) = z^{\deg R} R(1/z)$, using the fact that one of p^* and q^* (say p^*) is reciprocal, and the other (say q^*) satisfies $z^{\deg q^*} q^*(1/z) = -q^*(z)$. Now, for any $\varepsilon > 0$, apply Rouché's Theorem on the circle $|z| = 1+\varepsilon$, and let $n \to \infty$. This shows that $R(z) = (z^2 - z - 1)p - zq$ has at most one zero in $|z| > 1$. Also, R has no zeros on $|z| = 1$, as any such zero would also be a zero of R^*, and, as is easily checked, R and R^* are relatively prime. Finally, because one of $\{p(1), q(1)\}$ is zero and the other positive, in fact $R(1) < 0$, so that R does have one zero on $z > 1$.

□

Proposition 6. *Suppose that the pairs of polynomials $p_i, q_i \quad (i = 1, \ldots, I)$ each satisfy the circular interlacing condition. Then $\sum_i \frac{q_i(z)}{p_i(z)}$ is equal to a quotient $\frac{q(z)}{p(z)}$, where p and q also satisfy the circular interlacing condition.*

Proof. From Lemma 4 and the proof of Proposition 5(a), we know that for each i

$$\frac{z}{z^2-1} \cdot \frac{q_i(z)}{p_i(z)} = \sum_j \frac{\lambda_j}{x - \alpha_j} \tag{4}$$

where $x = z + 1/z$, the λ_j are positive, and the α_j are all real and in $[-2, 2]$. On adding, the same applies to $\sum_i \frac{z}{z^2-1} \cdot \frac{q_i(z)}{p_i(z)}$. Hence, by Lemma 4, this sum is equal to a positive scalar multiple of a quotient of polynomials $\frac{\prod_{j=1}^{d-1}(x-\beta_j)}{\prod_{j=1}^{d}(x-\alpha_j)}$, where $-2 \leqslant \alpha_1 < \beta_1 < \alpha_2 < \cdots < \beta_{d-1} < \alpha_d \leqslant 2$. Then on substituting $x = z + 1/z$ and considering separately the cases when $\alpha_1 = -2$ or $\alpha_d = 2$, we get the main result.

□

4. **The exponent of maximal torsion cosets**

As usual, let $\mathbb{G}_m$ denote the multiplicative group of $\mathbb{C}$. An *r-dimensional subtorus H* of $\mathbb{G}_m^n$ is a subgroup of the group $\mathbb{G}_m^n = \{(x_1, \ldots, x_n) \mid x_i \neq 0\}$ where, for some r, parameters $t_1, \ldots, t_r$ and integer matrix $E = (e_{ji})_{(j=1,\ldots,r;i=1,\ldots,n)}$ of rank r we have $x_i = t_1^{e_{1i}} \cdots t_r^{e_{ri}}$. It is an algebraic subgroup of $\mathbb{G}_m^n$, defined by the equations $\{\mathbf{x}^{\mathbf{a}} = 1 \mid \mathbf{a} \in A\}$, where the $\mathbf{a} \in A$ span the lattice of integer vectors orthogonal to the rows of E. A *torsion coset* is a translate $\boldsymbol{\omega}H$ of H by a torsion point $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n)$, the ω_i being roots of unity. An *exponent* of $\boldsymbol{\omega}H$ is any multiple of its order as an element of the group $\mathbb{G}_m^n/H$. A *maximal torsion coset* of a variety V is a torsion coset not properly contained in any other torsion coset in V. Results of Laurent [10, Th. 2], Bombieri and Zannier [3, Th. 2], and Schmidt [18, pp. 159–60] state that for any variety $V \subset \mathbb{G}_m^n$ defined over a number field K, the union of all torsion cosets contained in V is in fact contained in a union of finitely many maximal torsion cosets in V, with an upper bound for this number depending only on the parameters of K and V. Furthermore, in [18] Schmidt has given an explicit bound of this kind.

The finiteness of the number of maximal torsion cosets in V immediately implies the existence of a single exponent for all these cosets. This fact can be used to prove, as in

Section 6, that there are Salem numbers of a given trace, but without the upper bound on the smallest degree of such a number. The results that follow (Corollary 9 in particular) are needed to produce this degree bound.

We denote a typical torsion coset by $\mathtt{C} = \boldsymbol{\omega}\mathbf{t}^E = (\omega_i \prod_{j=1}^r t_j{}^{e_{ji}})_{(i=1,\ldots,n)} \subset \mathbb{G}_m^n$, E being an $r \times n$ integer matrix of rank r.

Consider a system of linear equations

$$\sum_{i=1}^{N} a_{\ell i} u_i = 0 \quad (\ell = 1, \ldots, L). \tag{5}$$

Following Schmidt, a solution $\mathbf{u} = (u_1, \ldots, u_N) \in \mathbb{G}_m^N$ will be called *nondegenerate* if there is no subset I of $\{1, \ldots, N\}$ with $0 < \#I < N$ such that

$$\sum_{i \in I} a_{\ell i} u_i = 0 \quad (\ell = 1, \ldots, L).$$

Lemma 7. *(see* [18, p. 168–9], [6] *) Suppose we have a nondegenerate solution of (5) where the u_i are all roots of unity. Then, up to a factor of proportionality, the u_i are all P_N -th roots of unity, where P_N is the product of all primes up to N.*

In fact, their result tells us that such solutions are m-th roots of unity, where m is the product of at most $2\sqrt{N}$ distinct primes $p \leqslant N$. However, we need an exponent valid uniformly for solution sets of different such N-term equations. This is why we take P_N-th roots of unity, P_N being the lcm of all such m. A uniform 'killer' exponent is provided by the following result, and its corollary.

Theorem 8. *Suppose that V is an affine variety in $\mathbb{G}_m^n$ defined over $\mathbb{Q}$, given say by polynomial equations*

$$\sum_{\mathbf{i}} a_{\ell \mathbf{i}} \mathbf{x}^{\mathbf{i}} = 0 \qquad (\ell = 1, \ldots, L) \tag{6}$$

with total degree d. Suppose also that the set

$$\mathcal{N}(V) = \{\mathbf{i} \in \mathbb{Z}^n \mid a_{\ell \mathbf{i}} \neq 0 \text{ for some } \ell\}$$

has diameter $D(V)$. Then every $(n-k)$-dimensional maximal torsion coset on V has an exponent mP_N for some integer $m \leqslant D(V)^{2k} k^{k/2}$. Here $N := \#\mathcal{N}(V) \leqslant \binom{n+d}{d}$.

Proof. The ingredients for the proof come from Schmidt [18]. Take $r = n-k$ and a maximal r-dimensional torsion coset $\mathtt{C} = \boldsymbol{\omega}\mathbf{t}^E$ on V, so that

$$\sum a_{\ell \mathbf{i}} \boldsymbol{\omega}^{\mathbf{i}} \mathbf{t}^{E\mathbf{i}} = 0 \quad (\ell = 1, \ldots, L).$$

Our aim is to find $\boldsymbol{\omega}_1$ with also $\mathtt{C} = \boldsymbol{\omega}_1 \mathbf{t}^E$, with $\boldsymbol{\omega}_1$ a vector of (mP_N)-th roots of unity for some $m \leqslant D(V)^{2k} k^{k/2}$. Now for any $\mathbf{j} \in \mathbb{Z}^r$ the coefficient of $\mathbf{t}^{\mathbf{j}}$ is

$$\sum_{\mathbf{i}: E\mathbf{i} = \mathbf{j}} a_{\ell \mathbf{i}} \boldsymbol{\omega}^{\mathbf{i}} = 0 \quad (\ell = 1, \ldots, L). \tag{7}$$

Here the sums over $\mathbf{i}$ are taken over all relevant $\mathbf{i}$ in $\mathcal{N}(V)$. Now (7) may be degenerate, splitting into nondegenerate equations

$$\sum_{\mathbf{i}\in I_q} a_{\ell\mathbf{i}}\boldsymbol{\omega}^{\mathbf{i}} = 0 \quad (\ell = 1,\dots,L, q \in Q \text{ say}) \tag{8}$$

for nonempty subsets I_q of $\mathbb{Z}^n$. Now, for a single q, apply Lemma 7 to (8), to obtain

$$\sum_{\mathbf{i}\in I_q} a_{\ell\mathbf{i}}\boldsymbol{\omega}^{\mathbf{i}-\mathbf{i}_q} = 0 \quad (\ell = 1,\dots,L) \tag{9}$$

where $\mathbf{i}_q$ is some fixed vector in I_q. Here, the number of terms is at most N . Then for all $q \in Q$, we have from Lemma 7 that all $\boldsymbol{\omega}^{\mathbf{i}-\mathbf{i}_q}(q \in Q)$ are vectors of P_N-th roots of unity.

Recalling that $k = n - r$, we claim that the set of all vectors $\{\mathbf{i} - \mathbf{i}_q \mid \mathbf{i} \in I_q, q \in Q\}$ generates a k-dimensional sublattice $\mathcal{L}_{\mathtt{C}}$ of $\mathbb{Z}^n$. For, from (7), the lattice $\mathcal{L}^E$ spanned by the rows of E is orthogonal to $\mathcal{L}_{\mathtt{C}}$, and so $\mathcal{L}_{\mathtt{C}}$ has dimension $\leqslant n-r$. But if the inequality were strict, there would be a nonzero vector $\mathbf{i}' \in \mathbb{Z}^n$ orthogonal to $\mathcal{L}_{\mathtt{C}}$ and not in the rational span of $\mathcal{L}^E$. Then for $\mathbf{i} \in I_q$ we would have $\mathbf{i}' \cdot \mathbf{i} = \mathbf{i}' \cdot \mathbf{i}_q$ (and also of course $E\mathbf{i} = E\mathbf{i}_q$), so for any $u \in \mathbb{G}_m$ we would have, for $\ell = 1,\dots,L$,

$$\begin{aligned}\sum a_{\ell\mathbf{i}}\boldsymbol{\omega}^{\mathbf{i}}\mathbf{t}^{E\mathbf{i}}u^{\mathbf{i}'\cdot\mathbf{i}} &= \sum_q \sum_{\mathbf{i}\in I_q} a_{\ell\mathbf{i}}\boldsymbol{\omega}^{\mathbf{i}}\mathbf{t}^{E\mathbf{i}_q}u^{\mathbf{i}'\cdot\mathbf{i}_q} \\ &= \sum_q \mathbf{t}^{E\mathbf{i}_q}u^{\mathbf{i}'\cdot\mathbf{i}_q}\sum_{\mathbf{i}\in I_q} a_{\ell\mathbf{i}}\boldsymbol{\omega}^{\mathbf{i}} \\ &= 0\,,\end{aligned}$$

and so the larger torsion coset $\boldsymbol{\omega}\mathbf{t}'^{E'}$ would lie on V, where $\mathbf{t}' = (\mathbf{t}, u)$ and $E' = \binom{E}{\mathbf{i}'}$, contradicting the maximality of $\boldsymbol{\omega}\mathbf{t}^E$.

Next take a basis $\boldsymbol{\ell}_1,\dots,\boldsymbol{\ell}_k$ of vectors in $\{\mathbf{i} - \mathbf{i}_q \mid \mathbf{i} \in I_q, q \in Q\}$ for $\mathcal{L}_{\mathtt{C}}$, and put $\boldsymbol{\omega} = e^{i\boldsymbol{\theta}} = (e^{i\theta_1},\dots,e^{i\theta_n})$. Write $\boldsymbol{\theta} = \sum_{j=1}^k \lambda_j\boldsymbol{\ell}_j + \boldsymbol{\psi}$, where $\boldsymbol{\psi} = \boldsymbol{\rho}E$ for some $\boldsymbol{\rho} \in \mathbb{R}^r$. Then, on solving the system of linear equations

$$\boldsymbol{\ell}_i \cdot \boldsymbol{\theta} = \sum_{j=1}^k \lambda_j \boldsymbol{\ell}_i \cdot \boldsymbol{\ell}_j \quad (i = 1,\dots,k)$$

and using the fact that $P_N\,\boldsymbol{\ell}_i \cdot \boldsymbol{\theta} \equiv 0 \pmod{2\pi}$ $(i = 1,\dots,k)$, we see that $P_N \det(\boldsymbol{\ell}_i \cdot \boldsymbol{\ell}_j)\boldsymbol{\lambda} \equiv 0 \pmod{2\pi}$. Note too that $\det(\boldsymbol{\ell}_i \cdot \boldsymbol{\ell}_j) \neq 0$. Then, using the Cauchy-Schwartz and Hadamard inequalities, we have that

$$|\det(\boldsymbol{\ell}_i \cdot \boldsymbol{\ell}_j)| \leqslant D(V)^{2k}k^{k/2}.$$

Put $\mathbf{t}_1 = e^{-i\boldsymbol{\rho}}$. Then $\mathbf{t}_1^E = e^{-i\boldsymbol{\psi}}$, and for $\boldsymbol{\omega}_1 = \boldsymbol{\omega}\mathbf{t}_1^E$ and some $m' = mP_N$ with $m \leqslant D(V)^{2k}k^{k/2}$ we have $\boldsymbol{\omega}_1^{m'} = 1$. Since

$$\mathtt{C} = \boldsymbol{\omega}\mathbf{t}^E = \boldsymbol{\omega}(\mathbf{t}_1\mathbf{t})^E = \boldsymbol{\omega}_1\mathbf{t}_2{}^E$$

say, we see that $\mathtt{C}$ has exponent m'. □

This result immediately gives us a killer exponent K valid for all maximal torsion cosets on V.

Corollary 9. *Let V be as in the Theorem, and $K = P_N \operatorname{lcm}(1, 2, \ldots, D(V)^{2n} n^{n/2})$, where $N = \#\mathcal{N}(V)$. Then every maximal torsion coset of V has exponent K.*

5. Maximal torsion cosets on a particular hypersurface

We shall be applying the results of the previous section to the affine hypersurface $h(\mathbf{x}) = 0$, where $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{G}_m^{n+1}$ and

$$h(\mathbf{x}) = 2(x_0^2 - 1)\prod_{i=1}^{n}(x_i - 1) - x_0 \sum_{j=1}^{n}(x_j + 1)\prod_{\substack{i=1 \\ i\neq j}}^{n}(x_i - 1).$$

The reason for looking at this hypersurface is that we shall apply the identity

$$\frac{h(\mathbf{x})}{2x_0 \prod_{i=1}^{n}(x_i - 1)} = \frac{x_0^2 - 1}{x_0} - \frac{1}{2}\sum_{i=1}^{n}\frac{x_i + 1}{x_i - 1}, \tag{10}$$

which is connected to our interlacing considerations of Section 3.

Lemma 10. *The only maximal torsion cosets of h with x_0 nonconstant are the algebraic subgroups B_{ij} of $\mathbb{G}_m^{n+1}$, where $i \neq j$ are both nonzero, and*

$$B_{ij} = \{\mathbf{x} \mid x_i = x_j = 1, x_0 = t_0, x_\ell = t_\ell (\ell \neq i, j)\},$$

of rank $n - 1$.

Proof. Clearly no point on $h = 0$ can have just one $x_i = 1$. If $\mathbf{x}$ with any two $x_i, x_j = 1$ is on $h = 0$ then it belongs to B_{ij}. Thus any other rank r maximal torsion coset with x_0 nonconstant has no x_i identically 1, so that we must have $x_0 = \omega_0 t_1^{e_{10}} \cdots t_r^{e_{r0}}$, where $(e_{10}, \ldots, e_{r0}) \neq 0$ and $x_i = \omega_i t_1^{e_{1i}} \cdots t_r^{e_{ri}}$, where $(e_{1i}, \ldots, e_{ri}) \neq 0$ whenever $\omega_i = 1$. By avoiding certain hyperplanes we can choose $\pm(k_1, \ldots, k_r) \in \mathbb{Z}^r$ not orthogonal to any nonzero $(e_{1i}, \ldots, e_{ri})$. Then for $(t_1, \ldots, t_r) = (t^{k_1}, \ldots, t^{k_r})$, $x_i = \omega_i t^{\ell_i}$ where $\ell_i := \sum_{j=1}^{r} k_j e_{ji} \neq 0$ when $\omega_i = 1$, and, by choice of the sign, $\ell_0 > 0$. Now as $t \to \infty$, the right-hand side of (10) goes to infinity, so that the coset cannot be on $h = 0$. □

We now estimate the killer exponent K, valid for every maximal torsion coset on this hypersurface, defined over $\mathbb{G}_m^{n+1}$.

Lemma 11. *There is a killer exponent K with $\log\log K < 0.2 + (3(n+1)/2)\log(n+3)$ for the hypersurface $h = 0$. Further, K can be chosen with all its prime factors less than $(n+3)^{3(n+1)/2}$.*

Proof. The hypersurface has diameter $D = \sqrt{n+4}$, degree $d = n + 2$, $N = \#\mathcal{N}(h = 0) = 3 \cdot 2^n$. Hence $D^{2n+2}(n+1)^{(n+1)/2} < (n+3)^{3(n+1)/2}$, and Corollary 9 gives $K = P_N \cdot \operatorname{lcm}(1, 2, \ldots, D^{2n+2}(n+1)^{(n+1)/2})$, with all prime factors of K less than $(n+3)^{3(n+1)/2}$.

Then, using standard bounds of Rosser and Schoenfeld [16] for the arithmetical functions θ, ψ we obtain

$$\begin{aligned}\log K &< \theta(3 \cdot 2^n) + \psi((n+3)^{3(n+1)/2}) \\ &< 1.02 \cdot 3 \cdot 2^n + 1.04 \cdot (n+3)^{3(n+1)/2} \\ &< 1.2(n+3)^{3(n+1)/2},\end{aligned}$$

giving the upper bound claimed. □

6. **Proof of Theorem 1**

The following lemma will complete the proof of Theorem 1.

Lemma 12. *For given even n there are positive integers $k_1, \ldots, k_n$ such that*

$$h(t, t^{k_1}, \ldots, t^{k_n}) = 2(t-1)^{n-1} S(t),$$

where $S(t) \in \mathbb{Z}[t]$ is monic irreducible and the minimal polynomial of a Salem number of trace $T := 1 - n/2$. Further, S has degree less than $\exp\exp(22 + 4T \log T)$.

Proof. For all maximal torsion cosets of h with x_0 constant (ie all except the B_{ij}) we can suppose that the constant x_0-values are all K-th roots of unity, where furthermore K has been chosen minimally. Note that K is certainly even, because the point $x_0 = x_1 = \cdots = x_N = -1$ lies on $h = 0$ and, as it is on no B_{ij}, must lie in one of the constant-x_0 maximal torsion cosets. Take $k_1 = K$, and $k_2, \ldots, k_n$ as the smallest $n-1$ primes not dividing K. Then all $k_1, \ldots, k_n$ are pairwise relatively prime. We now assert that for every root of unity ω and $\omega^{\mathbf{k}} = (\omega, \omega^{k_1}, \ldots, \omega^{k_n})$ with $h(\omega^{\mathbf{k}}) = 0$, we have $\omega = 1$.

For $\omega^{\mathbf{k}}$ belongs to some maximal torsion coset. If $\omega^{\mathbf{k}}$ has at least two components $= 1$, then (by the extended euclidean algorithm) $\omega = 1$. Alternatively, it belongs to no B_{ij}, and so to some maximal torsion coset with x_0 constant, $x_0 = \omega$, and so $\omega^K = \omega^{k_1} = 1$. This is impossible, as we cannot have just one $x_i = 1$, as noted above. This proves the assertion.

It is easy to check that $(d/dt)^n h(t, t^{k_1}, \ldots, t^{k_n})$ evaluated at $t = 1$, is nonzero. Furthermore, $h(t, t^{k_1}, \ldots, t^{k_n}) \equiv \prod_{i=1}^n (x_i - 1)(2(t^2-1) - tn) \equiv 0 \pmod 2$, so that all coefficients of h are even. This gives the stated factorization $2(t-1)^{n-1} S(t)$ of $h(t, t^{k_1}, \ldots, t^{k_n})$. Also, as all $k_i \geqslant 2$,

$$h(t, t^{k_1}, \ldots, t^{k_n}) = 2t^{2+\sum k_i} - nt^{1+\sum k_i} + \ldots$$

showing that $S(t)$ has trace $1 - n/2$.

Finally, to show that S is the minimal polynomial of a Salem number, observe that we have shown that none of its zeros are roots of unity. Now since $t^k + 1$ and $t^k - 1$ satisfy the circular interlacing condition, so does the sum $\frac{1}{2}\sum_{i=1}^n \frac{t^{k_i}+1}{t^{k_i}-1}$, by Proposition 6, so we can write it as $q(t)/p(t)$, where p and q satisfy the circular interlacing condition. Furthermore, as n is even, q has integer coefficients, as does $p = \prod_i (t^{k_i} - 1)/(t-1)^{n-1}$. Hence, as $p(1) = 0$, the numerator $S(t) = (t^2-1)p(t) - tq(t)$ of the right-hand side of (10) with $x_0 = t, x_i = t^{k_i}$ is, by Proposition 5(a), the minimal polynomial of a Salem number of trace $1 - n/2$.

Now the degree of S is $2+\sum_i k_i-(n-1)$, and from Lemma 11 we can take $k_2,\dots,k_n$ to be the smallest $n-1$ primes greater than $(n+3)^{3(n+1)/2}$. By Bertrand's Postulate (Chebyshev's Theorem), this gives $\deg S < K+(n-1)2^{(n-1)}\cdot(n+3)^{3(n+1)/2} < 2K$, and $\log\log\deg S < \log\log K+\log 2/\log K < 0.2+(3(n+1)/2)\log(n+3)+0.1$. For $n=2T+2$ one readily checks that this is less than $22+4T\log T$. □

Remark 13. There are many maximal torsion cosets with x_0 constant, for instance $x_0=-1, x_1=x_2^{-1}=t_1,\dots,x_{n-1}=x_n^{-1}=t_{n/2}$. Also one can for instance construct some for $x_0=1$ using the identity $3\cot\pi/3-\cot\pi/6=0$.

7. **Proof of Theorem 2**

Proof. The proof is much easier for Pisot numbers, as there are no possible cyclotomic factors to dispose of. We replace the fraction $(t^2-1)/t$ in (10) by $(t^2-t-1)/t$, and then can simply choose the parameters k_i to be the first n primes. Thus, again putting $\frac{1}{2}\sum_{i=1}^n \frac{t^{k_i}+1}{t^{k_i}-1} = q(t)/p(t)$, the polynomial $(z^2-z-1)p(z)-zq(z)$ will be the minimal polynomial of a Pisot number of trace $2-n/2$. □

8. **Computing Salem and Pisot numbers of negative trace.**

Salem and Pisot numbers of negative trace can be produced using $h(t,t^{k_1},\dots,t^{k_n})$, as in the previous sections. Thus, for the Pisot numbers of trace $-T$, the first $2T+4$ primes are used for the k_i. For the Salem numbers of trace $-T$, the first $2T+2$ primes are used for the k_i. In particular, k_1 is taken to be simply 2, instead of the very large killer exponent K used in the proof above. Computation using Maple shows that this produces a polynomial free of cyclotomic factors for $T\leqslant 25$, giving a Salem number of trace $-T$ and degree equal to the sum of the first $2T+2$ primes minus $2T-1$ (for instance degree 5540 for trace -25). However, we do not know whether this always happens. It would of course be nice if this could be proved, as we would then obtain a degree bound in Theorem 1 as good as that in Theorem 2.

Here is some pseudocode that gives the minimal polynomials. For a Salem number of trace $-T$:

$r=1; S=(z^2-1)(z-1); Q=z;$
`for` $j=1,\dots,T+1$ `do`
$q=$ `nextprime`$(r); r=$ `nextprime`(q);
$S=\frac{z^q-1}{z-1}\cdot\frac{z^r-1}{z-1}\cdot S-\frac{z^{q+r}-1}{z-1}\cdot Q;$
$Q=\frac{z^q-1}{z-1}\cdot\frac{z^r-1}{z-1}\cdot Q;$
`enddo`
`if` $\gcd(S(z),S(-z)S(z^2)S(-z^2))=1$ `then print`(S);
`endif`

The gcd condition tests for cyclotomic factors, and is based on the fact that a root of unity ω is conjugate to one of $-\omega$, ω^2 or $-\omega^2$. See [2] for further developments of this idea.

For instance, for $T = 2$ we obtain the (reciprocal) Salem polynomial

$$S_{-2}(z) = z^{38} + 2\,z^{37} - 2\,z^{36} - 19\,z^{35} - 57\,z^{34} - 123\,z^{33} - 222\,z^{32} - 357\,z^{31} - 527\,z^{30} - 727\,z^{29} - 950\,z^{28} - 1190\,z^{27} - 1440\,z^{26} - 1692\,z^{25} - 1936\,z^{24} - 2161\,z^{23} - 2355\,z^{22} - 2506\,z^{21} - 2602\,z^{20} - 2635\,z^{19} - 2602\,z^{18} - \cdots + 1$$

Note that the Salem polynomials S produced by this method have $|S(-1)S(1)|$ large. This is easily seen by putting $z = \pm 1$ in the pseudocode. An interesting question is whether there are Salem numbers with arbitrary trace and $|S(-1)S(1)| = 1$, the so-called *unramified* Salem numbers (see Gross and McMullen [8]).

For a Pisot number of trace $-T$:

$r = 1; P = z^2 - z - 1; Q = z;$
`for` $j = 1, \ldots, T + 2$ `do`
$q =$ `nextprime`$(r); r =$ `nextprime`(q)`;`
$P = (z^q - 1)(z^r - 1) \cdot P - (z^{q+r} - 1) \cdot Q;$
$Q = (z^q - 1)(z^r - 1) \cdot Q$`;`
`enddo`
`print`(P)`;`

Finally, we justify the statements in the Introduction. We note that there are Salem numbers of every nonnegative trace: for $n > 0$ the polynomial $z^4 - nz^3 - (2n+1)z^2 - nz + 1 = z^2((z+1/z)^2 - n(z+1/z) - (2n+3))$ is easily seen to be the minimal polynomial of a Salem number of trace n. This follows from the fact that $x^2 - nx - (2n+3)$ has one zero in $(-2, 2)$ and the other zero greater than 2. Also, $z^6 - z^4 - 2z^3 - z^2 + 1 = z^3((z+1/z)^3 - 4(z+1/z) - 2)$ is the minimal polynomial of a Salem number of zero trace.

The lower bound $\lfloor 1 - d/9 \rfloor$ for the trace of a degree $d \geqslant 10$ Salem number follows from the fact that the trace of a totally positive algebraic integer of degree $n \geqslant 5$ is greater than $16n/9$ ([13]) on noting that for a Salem number τ of degree d and trace $-T$, the number $\tau + 1/\tau + 2$ is totally positive of degree $d/2$ and trace $d - T$. Thus (turning the inequality around) for $-T \leqslant -2$ every Salem number of trace $-T$ has degree at least

$$2\left\lceil \frac{9T}{2} \right\rceil + 2 = \begin{cases} 18k + 2 \text{ for } -T = -2k \\ 18k + 10 \text{ for } -T = -(2k+1). \end{cases}$$

This inequality is sharp for $T = 2$ ([13]). The only Salem number of degree less than 10 having negative trace is the one with minimal polynomial $z^8 + z^7 - z^6 - 4z^5 - 5z^4 - 4z^3 - z^2 + z + 1$ ([19]).

Acknowledgment. We are grateful to the London Mathematical Society for their financial support for this work through a Collaborative Small Grant. We also thank the referee for helpful comments.

References

[1] Bertin, M.-J. ; Decomps-Guilloux, A. ; Grandet-Hugot, M. ; Pathiaux-Delefosse, M. ; Schreiber, J.-P., Pisot and Salem numbers. Birkhäuser Verlag, Basel, 1992.

[2] Beukers, F.; Smyth, C. J., Cyclotomic points on curves. Number theory for the millennium, I (Urbana, IL, 2000), 67–85, A K Peters, Natick, MA, 2002.
[3] Bombieri, E. ; Zannier, U., Algebraic points on subvarieties of $\mathbf{G}_m^n$. Internat. Math. Res. Notices 1995, 333–347.
[4] Boyd, David W., Small Salem numbers. Duke Math. J. 44 (1977), 315–328.
[5] Boyd, David W., Pisot and Salem numbers in intervals of the real line. Math. Comp. 32 (1978), 1244–1260.
[6] Conway, J. H. ; Jones, A. J., Trigonometric Diophantine equations (On vanishing sums of roots of unity). Acta Arith. 30 (1976), 229–240.
[7] Ghate, Eknath; Hironaka, Eriko. The arithmetic and geometry of Salem numbers. Bull. Amer. Math. Soc. (N.S.) 38 (2001), no. 3, 293–314.
[8] Gross, Benedict H.; McMullen, Curtis T., Automorphisms of even unimodular lattices and unramified Salem numbers. J. Algebra 257 (2002), 265–290.
[9] Hironaka, Eriko., The Lehmer polynomial and pretzel links. Canad. Math. Bull. 44 (2001), 440–451. Erratum: Canad. Math. Bull. 45 (2002), 231.
[10] Laurent, Michel, Équations diophantiennes exponentielles. Invent. Math. 78 (1984), 299–327.
[11] Mossinghoff,M., Online list of known small Salem numbers. `http://www.cecm.sfu.ca/~mjm/Lehmer/lists/SalemList.html`
[12] McKee, James, Families of Pisot numbers with negative trace. Acta Arith. 93 (2000), 373–385.
[13] McKee, James, Smyth, Chris, Salem numbers of trace -2 and traces of totally positive algebraic integers. Proceedings of the 6th Algorithmic Number Theory Symposium, University of Vermont 13 - 18 June 2004 (to appear).
[14] McKee, J. F. ; Rowlinson, P. ; Smyth, C. J., Salem numbers and Pisot numbers from stars. Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), 309–319, de Gruyter, Berlin, 1999.
[15] Reidemeister, K., Knot theory. Transl. from the German and ed. by Leo F. Boron, Charles O. Christenson, and Bryan A. Smith. (English) Moscow, Idaho, USA: BCS Associates. XV, 143 p. (1983). German: Knotentheorie. Reprint of 1932 original. Berlin-Heidelberg-New York: Springer-Verlag. VI, 74 S. (1974).
[16] Rosser, J. Barkley; Schoenfeld, Lowell, Approximate formulas for some functions of prime numbers. Illinois J. Math. 6 (1962), 64–94.
[17] Salem, Raphaël, Algebraic numbers and Fourier analysis. D. C. Heath and Co., Boston, Mass. 1963.
[18] Schmidt, Wolfgang M., Heights of points on subvarieties of G_m^n. Number theory (Paris, 1993–1994), 157–187, London Math. Soc. Lecture Note Ser., 235, Cambridge Univ. Press, Cambridge, 1996.
[19] Smyth, C. J., Salem numbers of negative trace. Math. Comp. 69 (2000), 827–838.

Department of Mathematics, Royal Holloway, University of London, Egham Hill, Egham, Surrey TW20 0EX, UK
E-mail address: `James.McKee@rhul.ac.uk`

School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland, U.K.
E-mail address: `C.Smyth@ed.ac.uk`